

1 Fred von Lohmann, Esq. (State Bar No. 192657)
Matthew J. Zimmerman, Esq. (State Bar No. 212423)
2 ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
3 San Francisco, CA 94110
Telephone: (415) 436-9333
4 Facsimile: (415) 436-9993
Attorneys for *Amicus Curiae*
5 Electronic Frontier Foundation

6
7
8 UNITED STATES DISTRICT COURT
9 FOR THE NORTHERN DISTRICT OF CALIFORNIA

10 ECHOSTAR SATELLITE LLC, et al.

11 Plaintiffs,

12 v.

13 FREETECH, INC and DOES 1-10,

14 Defendants.

Case No. 07-6124 (JW) (RS)

**AMICUS CURIAE BRIEF OF THE
ELECTRONIC FRONTIER
FOUNDATION IN SUPPORT OF
DEFENDANT FREETECH'S MOTION
FOR PROTECTIVE ORDER**

Date: September 15, 2008

Time: 9:30 a.m.

Dept.: Courtroom 4, 5th Floor, San Jose

1 The Electronic Frontier Foundation submits this *amicus curiae* brief in support of
 2 Defendant Freetech, Inc.'s ("Freetech") motion for a protective order relating to 17 subpoenas
 3 served by Plaintiffs Echostar Satellite LLC, Echostar Technologies Corp., and NagraStar LLC
 4 (collectively, "Echostar") on nonparty distributors of Freetech products on July 25, 2008 ("July 25
 5 Subpoenas") seeking the identities of every purchaser of Freetech's "Coolsat" free-to-air (FTA)
 6 satellite receiver.

7 STATEMENT OF INTEREST

8 The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization
 9 working to protect free speech and privacy rights in the online world. With more than 10,000
 10 dues-paying members, EFF represents the interests of technology users in both court cases and in
 11 broader policy debates surrounding the application of law in the digital age.

12 As part of its mission, EFF has intervened in a number of cases to protect the privacy
 13 interests of digital technology users targeted by overbroad discovery requests. For example, EFF
 14 has served as counsel or *amicus curiae* in cases involving the privacy interests of users of Internet
 15 search engines (*see Columbia Pictures Industries, Inc. v. Bunnell*, No. CV-06-01093-FMC (C.D.
 16 Cal. filed June 22, 2007) (*amicus curiae* brief addressing discovery request that would require an
 17 Internet search engine to create logs of user's search activities)), users of digital video recorders,
 18 (*see Paramount Pictures Corp. v. ReplayTV, Inc.*, No. CV-01-09358-FMC (C.D. Cal. filed May
 19 13, 2002) (*amicus curiae* brief addressing discovery request aimed at disclosing television viewing
 20 habits of owners of ReplayTV digital video recorders)), and anonymous contributors to Internet
 21 discussion forums (*see Doe v. 2themart.com, Inc.*, 140 F. Supp.2d 1088 (W.D. Wash. 2001)
 22 (served as counsel to resist discovery request aimed at revealing the identity of an anonymous
 23 speaker)). In addition, EFF recently brought user privacy concerns to the attention of Viacom in
 24 connection with discovery arising out of its ongoing copyright litigation against Internet video site
 25 YouTube. *See* Letter from Viacom General Counsel Michael Fricklas to Kurt Opsahl, July 15,
 26 2008¹ (addressing discovery request that would have disclosed viewing habits of YouTube users);

27
 28 ¹ Available at <<http://www.eff.org/deeplinks/2008/07/viacom-letter-eff-re-google-youtube-data-privacy>>.

1 John Boudreau, *YouTube, Viacom Agree to Mask Viewership Data*, S.J. MERCURY NEWS, July 16,
2 2008.²

3 The pending discovery dispute in this case not only concerns the parties and their
4 commercial partners but also jeopardizes the privacy interests of individual purchasers of
5 Freetech's FTA receivers. EFF files this *amicus curiae* brief in order to bring those interests to the
6 Court's attention.

7 ARGUMENT

8 **I. Introduction.**

9 This discovery dispute raises a question that reaches well beyond the commercial interests
10 of the parties: if an individual purchases a device that could be modified for unlawful uses, is that
11 individual's privacy forfeit when an aggrieved party later issues third-party discovery in a civil suit
12 against the device manufacturer? Here, in order to protect the important privacy interests of
13 entirely innocent purchasers of Freetech FTA receivers (*i.e.*, those who have *not* modified their
14 devices for unlawful uses), this Court should enter a protective order curtailing the scope of
15 Echostar's overbroad July 25 Subpoenas.

16 The July 25 Subpoenas seek the identities of individuals who have done nothing wrong.
17 Echostar admits that Coolsat receivers cannot intercept Echostar's encrypted television
18 programming unless they are modified with "Pirate Software." (Complaint ¶ 29.) Echostar's July
19 25 Subpoenas, however, seek names, addresses, phone numbers, and email addresses for *every*
20 purchaser of Coolsat receivers over the past 5 years, without regard to whether the purchasers have
21 made any "Pirate Software" modifications. Served on 17 nonparty distributors of Freetech
22 products, the subpoenas demand:

23 Documents sufficient to identify each Person who purchased or otherwise obtained
24 a Coolsat Receiver or Receivers from You during the period January 1, 2003 to June
25 30, 2008, including each Person's name, address, phone number, and email address,
and the purchase date, purchase price, purchase quantity, and model number for
each Receiver.

26 (Def. Br. at 4 and accompanying Golinveaux Decl. ¶ 4 & Exh. B.)

27
28 ² Available at <http://www.mercurynews.com/business/ci_9895989>.

As discussed further below, innocent purchasers of Freetech FTA receivers have good reason to fear having their identities revealed to Echostar. By Echostar's own admission, this litigation is part of a larger effort to crack down on what it perceives as widespread "piracy" of its television programming. (Complaint ¶¶ 32-35.) This raises the specter that Echostar will in the future threaten legal action against the individuals whose names it seeks in nonparty discovery here. In recent years, sophisticated commercial litigants — including satellite TV companies, record labels, and movie studios — have increasingly resorted to mass litigation against individuals in an effort to deter piracy. Unfortunately, innocent individuals have frequently been swept up in these litigation campaigns and found themselves with little recourse other than to pay thousands of dollars in "settlements" or face the even greater costs of civil litigation. In the words of a record industry spokesperson, "[w]hen you fish with a net, you sometimes are going to catch a few dolphin." See Dennis Roddy, *The Song Remains the Same*, PITTSBURGH POST-GAZETTE, Sept. 16, 2003.³

When viewed in this context, the danger to the privacy interests of innocent purchasers of Freetech devices is palpable. The pending motion for protective order may be the last opportunity for this Court to safeguard the interests those purchasers — once their names are disclosed to Echostar, there may be little that can be done to protect them from further harassment, legal threats, settlement demands, and associated legal costs.

II. The Discovery Requested by Plaintiffs Imposes an Unreasonable Burden on Innocent Purchasers of Freetech Devices.

This Court may "issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c). The exercise of this discretion is particularly appropriate in cases where overbroad discovery requests implicate the interests of nonparties. As this Court has previously recognized, "the word 'non-party' serves as a constant reminder of the reasons for the limitations that characterize third-party discovery." *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 680 (N.D. Cal. 2006) (quoting *Dart Indus. Co. v. Westwood Chem. Co.*, 649 F.2d 646, 649 (9th Cir.1980)). And where a subpoena is served on an

³ Available at <<http://www.post-gazette.com/columnists/20030914edroddy0914p1.asp>>.

1 intermediary that holds information about individuals, as here, a court may consider the privacy
2 interests of those individuals, as well as those of the subpoenaed intermediary. *Id.* at 687
3 (considering *sua sponte* the privacy interests of Google users in analyzing a discovery request to
4 Google seeking information about user's Internet searches).

5 The solicitude for the interests of nonparties is particularly justified where the nonparties
6 are individual citizens being drawn into litigation between sophisticated commercial entities. The
7 requirements of federal civil litigation impose special burdens on lay citizens who are often ill-
8 equipped to decipher subpoenas, requests for production, and interrogatories without the assistance
9 of counsel. Unlike commercial enterprises, which may have budgets for and relationships with
10 qualified counsel, individual citizens frequently lack these resources. *See, e.g., Theofel v. Farey-*
11 *Jones*, 359 F.3d 1066, 1074-75 (9th Cir. 2004) ("Fighting a subpoena in court is not cheap, and
12 many may be cowed into compliance with even overbroad subpoenas, especially if they are not
13 represented by counsel or have no personal interest at stake."). Here, Echostar has announced an
14 intention to contact the individuals whose identities it seeks in order to inquire into their uses of
15 Freetech's Coolsat receivers. (Def. Br. at 6 and accompanying Golinveaux Decl. at ¶ 5.)

16 Echostar's litigation here, however, imposes a more serious burden on innocent customers
17 than merely the burden of responding to further nonparty discovery. Where the allegations involve
18 "piracy" on the part of large numbers of individual technology users, innocent individuals have
19 special reason to be concerned. In recent years, federal courts have seen the rise of a new sort of
20 mass litigation, undertaken in the name of countering "piracy," where sophisticated commercial
21 entities threaten legal action against tens of thousands of individuals, often with disturbing
22 indifference to the fate of "dolphins" that may be caught up in the litigation dragnet.

23 In fact, this tactic of mass litigation against individuals was pioneered by the satellite
24 television industry. *See generally* Lauren McBraye, *The DirecTV Cases: Applying Anti-SLAPP*
25 *Laws to Copyright Protection Cease-and-Desist Letters*, 20 BERKELEY LAW & TECH. J. 603, 612-
26 14 (2005). Beginning in 2001, DirecTV, Echostar's chief competitor in the satellite television
27 market, obtained customer lists in the course of litigation against distributors of smartcard devices
28 that allegedly enabled signal piracy. *See Buckley v. DirecTV, Inc.*, 276 F. Supp. 2d 1271, 1273 n.2

(N.D. Ga. 2003) (“DirecTV obtained the identities of these individuals from customer lists seized pursuant to civil writs of seizure issued by United States District Court judges authorizing United States Marshals and DirecTV representatives to seize and impound products and related business records from individuals and companies designing, manufacturing, or trafficking in such equipment.”); Sylvia Hsieh, *DirecTV Sues Consumers Over Satellite Signal Theft*, LAWYERS WEEKLY USA, June 23, 2003.⁴ DirecTV then used those customer lists to deliver more than 170,000 letters demanding “settlements” of at least \$3,500 from each customer. *See DirecTV, Inc. v. Cavanaugh*, 321 F.Supp.2d 825 (E.D. Mich. 2003) (describing DirecTV demand letters); Declan McCullagh, *DirecTV Faces Setback in Dubious Antipiracy Campaign – Good*, CNET NEWS.COM, Sept. 12, 2007.⁵ DirecTV subsequently targeted individuals who did not capitulate in the face of the demand letter for litigation, resulting more than 24,000 suits in federal court. *See Blanchard v. DirecTV, Inc.*, 20 Cal. Rptr. 3d 385, 389 n.2 (Ct. App. 2004) (“At oral argument before this court, counsel for DIRECTV stated it could establish that, as of the summer of 2004, it had filed federal lawsuits against more than 24,000 individuals across the United States.”).

In the vast majority of these cases, DirecTV had no evidence that the individual in question had done anything other than purchase a device that *could have* been used to intercept DirecTV programming. *See DirecTV, Inc. v. Treworgy*, 373 F.3d 1124 (11th Cir. 2004) (rejecting DirecTV legal theory premised on mere possession of smartcards capable of interception); *DirecTV v. Cavanaugh*, 321 F.Supp.2d at 833 (“...DIRECTV has conceded, through its representative Larry Rissler, that the company has no direct evidence of signal interception.”). Not surprisingly, this overbroad targeting meant that DirecTV’s mass litigation campaign did a poor job separating the innocent from the guilty. Many of the smartcard devices targeted by DirecTV had perfectly lawful uses, yet many innocent purchasers swept up in DirecTV’s campaign were put in an impossible position — trapped between a settlement demand and the even higher costs of retaining counsel to establish their innocence.⁶ These defense costs were exacerbated by court rulings finding that

⁴ Available at <http://directvdefense.org/news/Lawyers_Weekly.pdf>.

⁵ Available at <http://news.cnet.com/8301-13578_3-9776790-38.html>.

⁶ Only after EFF and the Stanford Law School’s Center for Internet and Society took up the cause of the “dolphins” trapped in DirecTV’s net did the company reform its litigation campaign, agreeing not to threaten individuals in the absence of evidence of actual unlawful interception. *See*

1 evidence of mere possession of devices capable of interception was enough to create a triable issue
 2 regarding whether actual unlawful interception took place. *See, e.g., DirecTV v. Cavanaugh*, 321
 3 F.Supp.2d at 834. Trapped between a settlement demand and high defense costs, innocent
 4 individuals found themselves caught in what felt like a shake-down operation.

5 The parallels with the instant litigation are stark and troubling. The DirecTV experience
 6 makes palpable the jeopardy that innocent purchasers of Coolsat receivers face if their identities are
 7 disclosed to Echostar. And, as noted above, there is no reason to doubt that some if not most
 8 purchasers of Freetech's Coolsat receivers are entirely innocent. Echostar admits that Coolsat
 9 receivers are *incapable* of intercepting Echostar's programming without modification. (Complaint
 10 ¶ 29.) Even if some purchasers have modified their Coolsat receivers to intercept Echostar
 11 programming, that is no reason to compromise the privacy of those who have not, potentially
 12 putting them at risk of further entanglement in Echostar's anti-piracy campaign. In fact, the greater
 13 the proportion of Freetech customers who have modified their receivers, the greater the risk to
 14 those who did not — a conviction that “most of them are guilty” often drives indiscriminate
 15 enforcement efforts.⁷

16 The disclosure of customer lists, effected by seizure orders executed by U.S. Marshals,
 17 served as the initial kindling that started DirecTV's mass litigation campaign against individuals.⁸
 18 *See* Lauren McBraye, *The DirecTV Cases: Applying Anti-SLAPP Laws to Copyright Protection*
 19 *Cease-and-Desist Letters*, 20 BERKELEY LAW & TECH. J. at 613. In light of the DirecTV

20 EFF Media Release, *DirecTV to Narrow Anti-Piracy Campaign*, June 14, 2004, available at
 21 <<http://directvdefense.org>>.

22 ⁷ In fact, given the realities of the civil litigation process, this may be the last opportunity to
 23 protect the interests of innocent purchasers. Once their identities are handed over to Echostar,
 24 there may be no further judicial opportunity to stop Echostar from targeting customers *en masse*
 with demand letters, just as DirecTV did. In fact, when challenged in court over its demand letters,
 DirecTV successfully invoked the First Amendment and California's anti-SLAPP statute in
 defense of its right to send them. *See Blanchard v. DirecTV, Inc.*, 20 Cal. Rptr. 3d 385 (Ct. App.
 2004).

25 ⁸ The recording and movie industries are also conducting similar mass litigation campaigns that
 26 have, in the name of curtailing “piracy,” targeted more than 30,000 individuals for legal action.
 27 *See* Jeff Leeds, *Labels Win Against Song Sharer*, N.Y. TIMES, Oct. 5, 2007. These efforts have also
 28 been plagued by complaints from innocent individuals who have been swept up alongside those
 who have committed copyright infringement. EFF White Paper, *RIAA v. the People: Four Years*
Later, available at <http://w2.eff.org/IP/P2P/riaa_at_four.pdf>. However, in contrast to the satellite
 television context, those legal actions are the result of individualized investigations, rather than
 reliance on customer lists detailing the purchase of devices capable of lawful uses.

1 experience, innocent purchasers of Coolsat receivers have plenty of reason to fear Echostar's effort
 2 here to acquire customer lists through the more expedient mechanism of third-party subpoenas.
 3 Moreover, if approved by this Court, Echostar's use of nonparty discovery threatens to set a
 4 precedent that could imperil the privacy interests of consumers in still more contexts. To take just
 5 one example, many DVD players can be easily modified to ignore "region codes" embedded in
 6 DVD movies. *See, e.g.,* DVD Buying Guide, available at <<http://www.dvdbuyingguide.com/>>.
 7 The motion picture industry has sued DVD player manufacturers for failing to make DVD players
 8 "robust" against these modifications. *See* Marc Perton, *Samsung Sued Over DVD-Duping by*
 9 *Discontinued Player*, ENGADGET, Feb. 20, 2006.⁹ Would the motion picture studios be entitled, in
 10 their litigation against DVD player manufacturers, to propound discovery to every retailer seeking
 11 the identities of every customer who purchased any DVD player later discovered to be "hackable"?
 12 To permit Echostar to succeed in its overbroad discovery request here threatens to open a
 13 Pandora's Box for consumers of digital devices. Because Echostar's July 25 Subpoenas impose an
 14 undue burden on the privacy interests of Coolsat purchasers and also have the potential to inflict
 15 substantial annoyance and harassment on them, this Court should take this opportunity to prevent
 16 this abuse of the discovery process.

17 **III. Plaintiffs Have Alternate, Less Intrusive Means to Obtain Relevant Evidence.**

18 The Court should also grant Freetech's motion for a protective order because the July 25
 19 Subpoenas seek information that is not necessary to Echostar's Digital Millennium Copyright Act
 20 ("DMCA") claims.¹⁰ "[A] district court may in its discretion limit discovery on a finding that the
 21 discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other
 22 source that is more convenient, less burdensome, or less expensive." *Gonzales v. Google*, 234
 23 F.R.D. at 686 (quoting Fed. R. Civ. P. 26(b)(2)(i)). "*Even if relevant*, discovery is not permitted
 24 where no need is shown, or compliance would be unduly burdensome, or where harm to the person
 25 from whom discovery is sought outweighs the need of the person seeking discovery of the

26
 27 ⁹ Available at <<http://www.engadget.com/2006/02/20/samsung-sued-over-dvd-duping-by-discontinued-player/>>.

28 ¹⁰ Echostar has made no effort to establish that customer identity information is relevant to any of its other claims. (Def. Br. at 6 n.2.)

information.” *Micro Motion, Inc. v. Kane Steel Co.*, 894 F.2d 1318, 1323 (Fed. Cir. 1990) (emphasis in original).

According to Echostar, “customer information is necessary for Plaintiffs to conduct a survey analysis on the issue of whether Defendant’s FTA receivers are primarily being used for the piracy of Plaintiffs’ DISH network satellite signal, as opposed to receiving and viewing purely free-to-air television programming.” (Def. Br. at 6 and accompanying Gollinveaux Dec. ¶ 5.) In focusing on the “primary use” of Coolsat receivers, Echostar is presumably referring to its DMCA claims pursuant to 17 U.S.C. § 1201(a)(2) and (b)(1):¹¹

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) *has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title*; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

17 U.S.C. § 1201 (a)(2)(B) (emphasis added).¹²

The disjunctive “or” linking subsections (A), (B), and (C) makes it clear that liability can be premised on a showing under any of the three subsections. Echostar’s complaint specifically alleges that Freetech’s Coolsat receivers (or components thereof) were primarily designed for circumvention (subsection (A)), as well as marketed for circumvention (subsection (C)). (Complaint ¶¶ 36-41.) If Echostar is able to prove these allegations, which would not require intrusive, indiscriminate discovery against all Coolsat purchasers, it will have proven its case under

¹¹ Echostar also proceeds under 17 U.S.C. § 1201(b)(1)(B), which prohibits trafficking in technologies that enable circumvention of “copy controls” that restrict *use* of a copyright work after lawful *access* has been granted. See 3 NIMMER ON COPYRIGHT § 12A.03[C] & [D]. The language and structure of § 1201(b)(1)(B) is identical to the language of § 1201(a)(2)(B) in all respects relevant to the pending motion.

¹² Congress made it clear when passing the DMCA that these provisions were “drafted carefully to target ‘black boxes,’ and to ensure that legitimate multipurpose devices can continue to be made and sold.” H.Rep. 105-551, Part 1, 105th Cong., 2nd Sess., at 18 (1998), available at <http://www.hrrc.org/File/HRept_105-551_May_22_.pdf>.

1 § 1201(a)(2) and/or (b)(1). In short, it appears that customer identities may be entirely unnecessary
2 to Echostar's DMCA claims.

3 Even if Echostar were unable to muster sufficient evidence regarding the design and
4 marketing of the Freetech devices, there are other avenues by which Echostar can develop its case
5 under subsection (B) regarding the "commercially significant purpose or use" of the Coolsat
6 receivers. Echostar can retain experts to examine the FTA receiver industry, comparing the
7 Coolsat receiver against competing receivers that are more difficult (or easier) to modify for
8 unlawful interception. This evidence could also be supplemented by materials gathered on the
9 Internet forums and websites that Echostar describes in its Complaint. (Complaint ¶¶ 32-34, 43.)
10 Based on Echostar's allegations, it appears that there is no shortage of Coolsat owners who readily
11 discuss in such forums their modification of the receivers for unlawful interception. (Complaint ¶
12 33-34.) In short, there has been no showing that innocent purchasers, who have not made
13 modifications to their receivers, must be drawn into this litigation in order to afford Echostar its
14 full day in court.

15 CONCLUSION

16 For the foregoing reasons, the Court should grant Freetech's motion for a protective order
17 and require that Echostar modify its July 25 Subpoenas in order to prevent the wholesale disclosure
18 of customer lists identifying individuals who purchased Coolsat receivers.

19
20 DATED: August 15, 2008

21 By /s/

22 Fred von Lohmann, Esq. (State Bar No. 192657)
23 Matthew Zimmerman, Esq. (State Bar No. 212423)
24 ELECTRONIC FRONTIER FOUNDATION
25 454 Shotwell Street
26 San Francisco, CA 94110
27 Telephone: (415) 436-9333 x123
28 Facsimile: (415) 436-9993

Attorneys for *Amicus Curiae* Electronic Frontier
Foundation